Middle East Journal of Applied Science & Technology
Vol.5, Iss.2, Pages 201-209, April-June 2022

A Comprehensive Review on Data Security and Threats for Data Management in Cloud Computing

Dr. Satinderjeet Singh*

Associate Manager – The Children's Place, 500 Plaza Drive, Secaucus, New Jersey, USA – 07094.
Email: drsatinderjetsingh@gmail.com

DOI: http://doi.org/10.46431/MEJAST.2022.5220

Article Received: 27 March 2022 *Article Accepted: 25 June 2022* *Article Published: 30 June 2022*

ABSTRACT

The cloud is a network of virtual computers that are linked together and may exhibit and offer computational capabilities continuously depending on certain Service Level Agreements (SLAs) that have been agreed between the parties to a contract between the clients and the internet provider. Cloud computing has several benefits, including endless computational resources, cheap cost, security controls, hypervisor protection, instantaneous elasticity, high throughput, and fault-tolerant solutions with increased performance. Since cloud computing is a comparatively recent computing model, there exists a lot of uncertainty about how well confidentiality of all levels, including host, network, data levels, and implementation, can be achieved. As a result, there still are important obstacles to cloud computing adoption. These constraints include security issues concerning privacy, compliance, and legal issues. When databases and software applications are moved from the cloud to large data centers, data management becomes a major challenge. Numerous security issues may develop while using cloud computing, including issues with privacy and control, virtualization and accessibility issues, confidentiality, management of credentials and identities, authentication of responding devices, and authenticity. In this paper, an effort is made to offer a comprehensive review of data security and threats in cloud computing.

Keywords: *Cloud computing, Data management, Computational resources, Authentication, Confidentiality, Data security.*

1. Introduction

The development of guidelines and recommendations for cloud computing systems is the responsibility of NIST, which contributes a significant amount toward improving knowledge of cloud services and software applications. Public, private, community, and hybrid clouds are the four main methods that make up the cloud computing infrastructure [1-3]. The deployment models show how the cloud servers may be used to be delivered by the data centers [4]. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service are the three cloud service architectures or delivery types that are offered to the user. For these service models in the cloud infrastructure, several security levels are necessary. The broad selection of services that are taken into account in the cloud's fundamental characteristics layer and is accessible via the internet. The goal of the cloud service provider is to monitor resource allocation, deliver services, and maintain security [5-8].

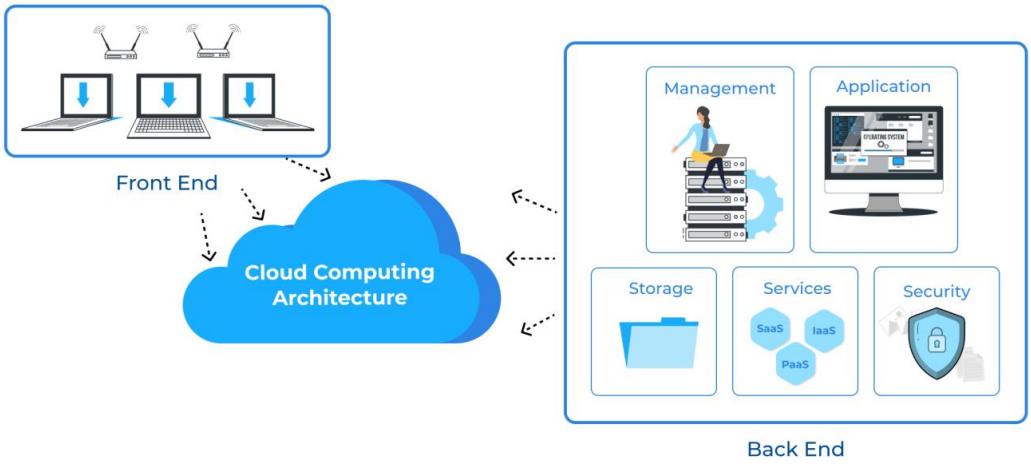

Figure 1. Cloud computing Architecture

The framework uses the five fundamental parts, which are made up of cloud services. When available resources or data are transferred to the cloud using a client-server architecture, cloud security is a crucial and challenging issue [9]. Figure 1 depicts the cloud computing framework.

1.1. Deployment Models in Cloud Infrastructure

The cloud computing environment defines the characteristics and function of the cloud and contains three deployment models that can be utilized in specific to depict the cloud service models [10]. The deployment models are categorized as follows and may be seen in Figure 2.

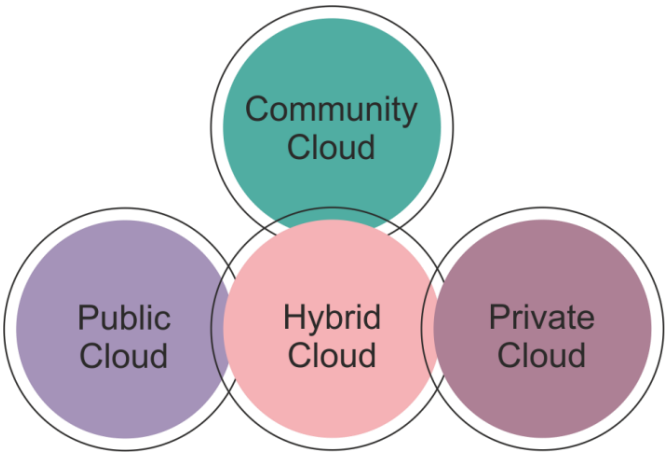

Figure 2. Deployment models in the cloud environment

(a) Public Cloud: A public cloud is managed by the network operator, hosts data in the cloud, and has service-level agreements between the user and the service provider. Cloud service providers include Microsoft, Google, Amazon, VMware, IBM, Sun, and Rackspace, to name a few. The infrastructure is created using a generalized computing model that accommodates all common client demands. The information is easily accessible and made available to a broader audience. The operation of public clouds involves several organizations, and because the resources are accessible to consumers, it is challenging to keep them safe from malicious assaults. Because it is out of the firewall, there are certain problems with consumer security, data services, and security. It is less secure as compared to other deployment options and is suitable for small and medium-sized businesses which do not need to buy capital equipment or set up servers.

(b) Private cloud: Multiple clients are served by one company that manages and maintains the cloud platform. Any company that previously installed its physical hardware servers with a virtual layer atop and set up its own private cloud will only render resources that are available locally. They do not have to use Microsoft or Amazon servers because their program can be deployed to their own physical control server. They will build their whole infrastructure from scratch. Due to its unique local exposures, this can guarantee protection and is more secure than a public cloud. The only access available for use by the specified stakeholders and organization is the private cloud. Nevertheless, the price is substantially greater since the server administrator, virtualization specialist, and network specialist all require specialized expertise and training. Clients can utilize and exchange the virtual applications and scalable resources that the cloud service provider has gathered together. Since the platform is controlled and operated by the same company, it is simpler to resolve the relationship between the provider and the client in private

clouds. Private clouds use the functionalities of cloud management software to guarantee dependable delivery service and integrity of external information.

(c) Hybrid Cloud: A hybrid cloud is a combination of two or more cloud deployment methods, which may be public, private, or community clouds that still stay separate, independent entities. When a client has a large requirement for resources, hybrid clouds are important because they often permit the migration of certain computing tasks from private to public clouds. Since it provides more secure control over the programs and information, it is well-structured and enables data to be accessed by many parties over the network. It has advantages over other deployment techniques and may be handled both inside and outside. The hybrid cloud is becoming ever more common and is already the standard. The main reason is that it could benefit from cost-saving, scalability, and flexibility that public clouds may offer, as well as flexibility in management, whenever required.

(d) Community Cloud: A community cloud is when an organization shares its cloud platform with clients who have a common interest or set of issues, such as those related to policy, security needs, purpose, and accountability. The resources of the community cloud are managed, supervised, shared, and operated by many organizations or third parties. In the event that a third party, such as Siemens, offers IT products and solutions, the media cloud might be set up. It is often more uncommon and specialized. The cloud infrastructure of the community cloud is used and controlled by a variety of organizations, including research groups, businesses, and governmental agencies.

2. Security Threats in Cloud Computing

Data security and cloud security are getting importance, and several large corporations are developing policies and procedures to address security issues. Governments have been compelled to enact new laws and regulations in response to the rising and persistent security vulnerabilities, which have made cybersecurity and privacy issues a top priority [11-12]. Small- and large-scale businesses, as well as the public and private industries, are required to adhere to regulatory guidelines and regulations to protect digital assets' accessibility, confidentiality, and integrity [13-14]. Infractions of these security breaches carry severe consequences. At the corporate level, encryption and encoding are essential for improved security.

Cloud security concerns are a significant barrier to adoption. Sensitive information accessibility, data segmentation, security, bug exploits, recoveries, ownership, malicious users, control console security, access controls, and multi-tenancy difficulties are examples of security challenges that can be categorized. To increase client confidence in cloud computing technologies, several additional risks and obstacles might result in security breaches.

2.1. Security and Privacy

The crucial concepts in cloud computing security are cryptography techniques and policy rules, and therefore both require a significant amount of consideration. Since recent research areas are required to improve current cryptographic techniques for cybersecurity, privacy protection, and outsourcing computation [15]. Because clients' confidential and vital data is stored in the cloud, security and privacy are seen as significant issues in an environment of cloud computing. Since data is sent outside of businesses' local area networks, some claim cloud computing is not safe. Since it incorporates many various technologies for its capabilities and implementation, such as networks, operating systems (OS), database systems, virtual servers and elements, bandwidth allocation,

transactions, parallel processing techniques, load balancing, memory allocation, and many others, cloud computing is not a dedicated hardware computing platform. As a result, a risk to any of these technologies affects the whole cloud platform. Because of this, implementing the SaaS distribution model presents a significant security problem.

(a) Privileged access: Due to problems with information security, data handled beyond organizations is vulnerable to several threats. Businesses must question their suppliers for further information regarding who has access to sensitive data and who oversees the administrators' recruitment and supervision.

(b) Data separation: The majority of cloud services store data in a communal setting. As a result, a company needs to set up a system to isolate customer information. Not all information is encrypted, and some software errors might lead to attacks or security breaches. Users should be aware of whom has access to the decryption keys or what portions of the information each key can decode.

2.2. Security threats with SaaS

In SaaS, the customer must rely on the provider to implement adequate security principles. To prevent additional consumers from viewing one another's data, the service provider must take the necessary steps. Therefore, it becomes challenging for the user to confirm that the appropriate security precautions have been taken and that the program will be available when necessary. SaaS, offer on-demand access to corporate programs including ERP, CRM, and SCM as well as mail and conference software. SaaS users have little management over privacy than clients of the other three major cloud delivery types. SaaS application deployment can cause certain security issues.

3. Classification of Data Security Issues

All platforms share the problem of data security. If used in an unregulated context like cloud services, it poses a serious difficulty. It is essential to differentiate between security concerns brought on by using cloud technology and those connected to all IT systems [16-17]. Open, shared, and distributed settings are typically linked with these vulnerabilities. To properly assess the dangers, it is crucial to distinguish between current issues and those caused by cloud services. In this study, we exclusively address problems brought through the cloud and information. Because it is kept on the system of the service provider, is easily accessible via the internet, and is shared with other clients, data saved on network infrastructure is more prone to security threats than information stored on the traditional system. Despite the numerous ways to categorize information security challenges, here we group them into three categories, as illustrated in Figure 3 as single Cloud characteristics, Cloud data life cycle, and information security attributes. The goal is to draw attention to the way these factors affect information security in addition to the general and specific information security consequences connected to these classifications.

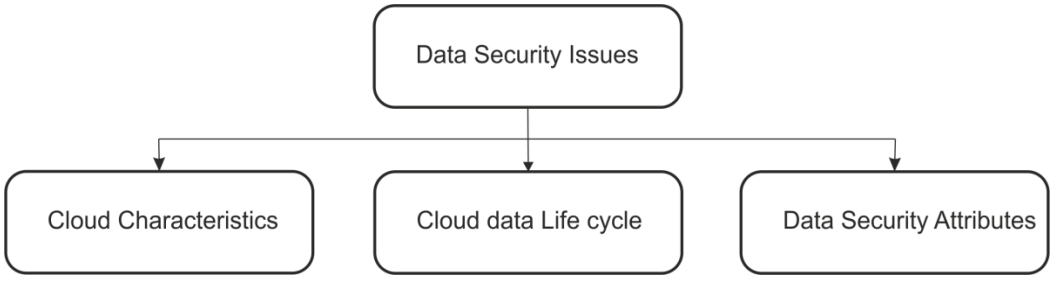

Figure 3. Taxonomy of Cloud data security issues

3.1. Cloud Characteristics

In this section, considerations are made with the data security concerns that the differences between conventional commercial architecture and cloud architecture raise. Architecture in the cloud is distinct from the structure in the traditional sense. While these distinctions have so many advantages, they also bring up a lot of inconveniences that might compromise security. The following are the key traits, immediate advantages, and inconveniences: Facilities that have been leased–Cloud architecture now pertains to the service provider rather than the user. Customers rent the usage of the hardware platform from a service provider rather than buying it outright. The main benefit is cost savings. The main inconvenience is losing control. Open infrastructure - Connectivity to cloud architecture often occurs online. The main benefit is that services are accessible anywhere. Several entrance options are the primary inconvenience. Cloud infrastructure is accessed by service users, in contrast to dedicated conventional infrastructure. The main benefit is cost savings. Risks of isolating failures among customers are the main inconvenience. Elastic infrastructure enables consumers to scale up and down services based on their needs. As a result, the cloud platform scales to meet current demands, as contrasting to conventional architecture, which is dependent on peak usage. Optimizing the consumption of resources is the main benefit. Reallocation risks for resources are the main inconvenience. Architecture that has been virtualized – The Cloud's fundamental idea is virtualization. The physical machine is no more used; instead, we discuss about the virtual machine. Optimizing infrastructures is the main benefit. The main inconvenience is the standard virtualization issues. Infrastructure that is geographically distributed throughout the world makes up the cloud. Increased computing and storage capacity is the main benefit. Infrastructure management and maintenance are the biggest inconveniences. All these traits affect information security.

4. Data Security in Cloud Computing

Data encryption is only one aspect of data security in the cloud. Data protection requirements differ based on the three service models, such as SaaS, PaaS, and IaaS. Such three stages of data—Data at Rest also refers to information that is stored in the cloud, Data in Transit refers to information that is going into the cloud, and Data in Use refers to information that is used in and out of the cloud—all pose potential risks to the cloud's data. The characteristics of data procedures, protection measures, and procedures determine the privacy and integrity of the information. Three states contain (Figure 4):

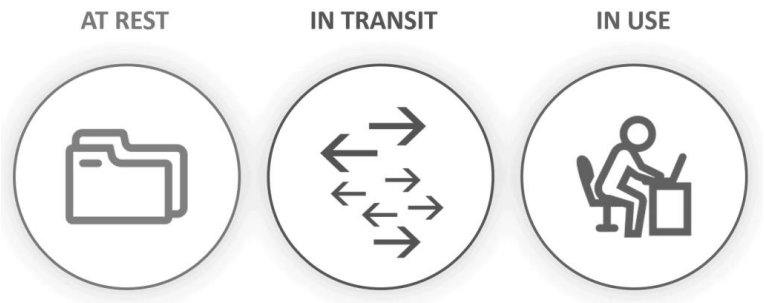

Figure 4. Three stages of data

(A) Data at Rest - Whatever information is accessed via the web is considered to be at rest, including information stored in the cloud. This includes both existing information and backup data. Therefore, considering that they

do not already have physical control over the data, organizations find it very difficult to safeguard data at rest if they do not manage cloud infrastructure. So, by keeping a private cloud with strictly restricted access, this vulnerability may be identified.

(B) Data in transit - Data in transit refers to information that is entering and exiting the cloud. This information may be applied for usage at certain positions and could be kept as documents or databases in the cloud. Data that is transferred to the cloud is referred to as data in transit. Account names and passwords are much more sensitive information that sometimes could be encrypted. Data in transit, therefore, include information in plaintext form. Since it needs to move from one location to the other, data in transit is more susceptible to dangers than data at rest. The information can be inspected by intermediate software in a variety of ways, and it occasionally has the power to modify the information as it travels to its final location. Encryption is a key component of the main strategies for data security in transit. Figure 5 displays the data in transit and at rest.

(C) Data-in-use - Management of data in use, such as creation, alteration, and destruction. Because of the large number of clients participating in the cloud infrastructure, while processing occurs there are additional risks of mistreatment.

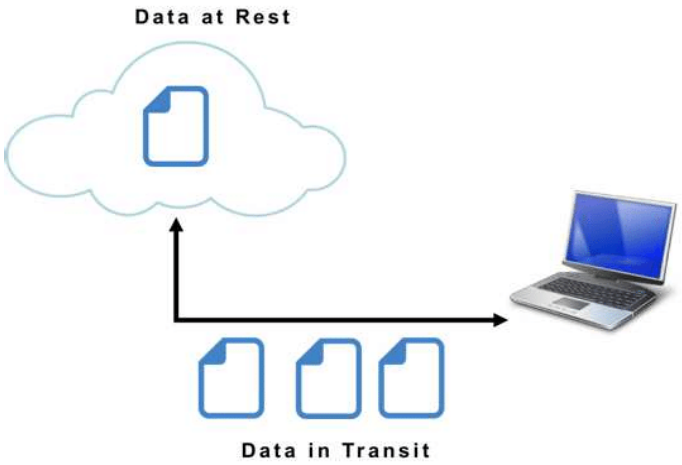

Figure 5. Data in rest and transit

In the Platform as a Service (PaaS) approach, in addition to the services provided by IaaS, the CSP allows developers to build a platform. A development platform is provided by the CSP, over which programs may be created. In other terms, instead of installing programming tools on their computers, development teams may create their applications using a virtual platform that is available through an Internet browser. The programmers may simply share or distribute their software to the cloud as a result. It is best to think of this solution as a cloud OS to prevent any misunderstanding with SaaS. Consumers of the system are given the option by the company's administrators to deploy their apps on an infrastructure that can run any software or indeed imitate different types of hardware. Service-based software (SaaS) is a highly well-liked service wherein providers of cloud services distribute computer programs online. When a user requests it, a SaaS provider will install its software that is either housed in its own data center or on hardware from some other provider. Programs may be licensed explicitly to an organization, set of users, a client, or via a private entity that handles numerous licenses across user organizations, such as an ASP. This procedure is often carried out through a licensing model. The client also may use any

clearly-specified Internet device, more likely an Internet browser, to retrieve the apps. Models for cloud services are another name for such building components.

Working with innovative private cloud computing providers in some kind of way that does not compromise the privacy of the company is a reasonable way to make use of cloud computing's benefits. An excellent cloud-based security system has the five following benefits:

1. Defense from DDoS: Distributed denial-of-service attacks are rapidly increasing, and a leading cloud-based security plan focuses on methods to prevent massive volumes of data headed for a company's data centers; reducing risk, involves monitoring, storing, and disseminating DDoS attacks.

2. Data security: A leading cloud computing secure system features security requirements designed to safeguard sensitive information and transfers in the continuously rising age of information breaches. This prevents a third party from secretly hearing in or tampering with the transferred data.

3. Regulatory compliance: The best cloud computing security systems assist firms in targeted projects by managing and maintaining the updated framework for consistency and safeguarding personal and financial data.

4. Flexibility: Whether it is needed to turn up or down the restriction, a cloud computing solution gives the required protection. Upgrading the cloud setup gives the ability to avoid server breakdowns in periods of high demand. Whenever the peak period of heavy traffic has passed, companies may scale back to save costs.

5. High support and availability: A security plan for cloud technology that follows standard methods provides ongoing assistance for an organization's advantages. This includes ongoing observation throughout the year, twenty-four hours a day, seven days a week. To ensure that the website and applications of the company are online at all times, redundancy is built in.

Companies may run their operations in a global business center with the availability, consistent quality, and security provided by an upper-edge secure cloud computing framework. The physical structure is combined with advanced cybersecurity features to provide higher security features.

5. Conclusion

Initially, both businesses and academics utilized interfaces to communicate with computer systems, which were frequently located far away. These interfaces did not have any computational power originally. The goal was to reduce the usage of such expensive computer systems more expense by distributing their capabilities, such as CPU time, across several users. Cloud computing refers to the type of service that a network operator offers. The customer of these services is not required to understand or be concerned regarding how the services are offered or managed (e.g., network, memory, applications). However, the client simply cares that the solution will be offered anytime they require it. The use of cloud computing frees businesses from the requirement for their data centers. It saves money on equipment, cooling systems, memory, and power supply purchases, maintenance, and upgrading. As a consequence, using cloud computing helps businesses to easily grow existing operations and launch new ventures swiftly. To provide a better alternative for cloud settings, a thorough examination of data security and threats in cloud computing is systematically conducted in this work.

Declarations

Source of Funding

This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The author declares no competing financial, professional, or personal interests.

Consent for publication

The author declares that he/she consented to the publication of this research work.

References

[1] Ali M., Khan SU., Vasilakos AV. (2015). Security in cloud computing: opportunities and challenges. Inf Sci., 2015: 357–383.

[2] AlShehri MAR., Mishra S. (2019). Feature based comparison and selection of SDN controller. Int J Innov Technol Manag., 16(05): 1–23.

[3] Avram MG. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. Procedia Technol., 2014: 529–534.

[4] Bellini P., Cenni D., Nesi P. (2015). Smart cloud engine and solution based on knowledge base. Procedia Comput Sci., 2015: 3–16.

[5] De Oliveira AS. (2018). Modelling trust and risk for cloud services. J Cloud Comput., 7(1): 7–14.

[6] Chen HC., Lee PP. (2013). Enabling data integrity protection in regenerating-coding-based cloud storage: theory and implementation. IEEE Trans Parallel Distrib Syst., 25(2): 407–416.

[7] Coppolino L., D'Antonio S., Mazzeo G., Romano L. (2017). Cloud security: Emerging threats and current solutions. Comput & Electr Eng., 2017: 126–140.

[8] Hong JB., Nhlabatsi A, Kim DS., Hussein A., Fetais N., Khan KM. (2019). Systematic identification of threats in the cloud: A survey. Comput Netw., 2019: 46–69.

[9] Benabied, S., Zitouni, A., & Djoudi, M. (2015). A cloud security framework based on trust model and mobile agent. In 2015 International Conference on Cloud Technologies and Applications, pp. 1–8.

[10] Abusaimeh, H. (2020). Security Attacks in Cloud Computing and Corresponding Defending Mechanisms. International Journal of Advanced Trends in Computer Science and Engineering, 9(3).

[11] Dheyab, O. A., Turki, A. I., & Rahmatullah, B. (2018). Threats and Vulnerabilities Affecting the Adoption of Cloud Computing in Iraq. The Journal of Social Sciences Research, pp. 599–606. DOI: 10.32861/jssr.spi6.599.606.

[12] Jamil, D., & Zaki, H. (2011). Security issues in cloud computing and countermeasures. International Journal of Engineering Science and Technology (IJEST), 3(4): 2672–2676.

[13] Abdul-Jabbar, S. S., Aldujaili, A., Mohammed, S. G., & Saeed, H. S. (2020). Integrity and Security in Cloud Computing Environment: A Review. Journal of Southwest Jiaotong University, 55(1).

[14] De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from clouds: Security of cloud computing in the IoT era. Future Internet, 11(6): 127. DOI: 10.3390/fi11060127.

[15] Qi, Q., & Tao, F. (2019). A smart manufacturing service system based on edge computing, fog computing, and cloud computing. IEEE Access, 7: 86769–86777. DOI: 10.1109/ACCESS.2019.2923610.

[16] Kaur, R., & Kinger, S. (2014). Analysis of security algorithms in cloud computing. International Journal of Application or Innovation in Engineering & Management, 3(3): 171–176.

[17] Singh, J. (2014). Cyber-attacks in cloud computing: A case study. International Journal of Electronics and Information Engineering, 1(2): 78–87.